IERG 4210 Tutorial 2 - Phase 2A

Secure Server Setup

Xiao Yi modified according to previous TA **Siyue Xie**'s slides

yx019@ie.cuhk.edu.hk

Outline:

- Amazon Web Service and EC2 Instance
- Environment Setup
  - LAMP (Linux, Apache, MySQL, PHP/Perl/Python)
  - We will discuss the database in the following tutorials
- Security Configurations

1. Amazon Web Service (AWS)

AWS provides the 12-month free EC2 instance for every newly registered user. If you have already used up your free quota, you can register using a new email address. Please check the following links:

AWS Free Tier: https://aws.amazon.com/free AWS Sign-up: https://portal.aws.amazon.com/billing/signup#/start

1.1 Create EC2 Instance

1. Enter the EC2 console and select **Instance** in the side panel
2. Click **Launch Instance**
3. Select a free tier image, e.g., **Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type**, and choose **t2.micro**
4. Confirm and Launch
5. **Important: Save the private key to your local machine!!!**

1.2 Remote Access via SSH

1. Elastic IP
   1. Select **Elastic IP** in the side panel and
   2. Click **Allocate Address** and confirm
   3. Associate the IP address to the EC2 instance
2. Open **Terminal**, or other SSH tools, e.g., Putty (Windows), Xshell (Windows), and Royal TSX (Mac)
3. Type the following command to connect:

   ```
   ssh -i "xxx.pem" ec2-user@[server IP address]
   ```

   Where `"xxx.pem"` is the path to your private key, and `[server IP address]` is the Elastic IP address of your EC2 instance

Potential Problems:

- Set permission for your private key (on the local machine):

```
chmod 400 xxx.pem
```

- For Putty users: convert `.pem` key file into `.ppk` key file by **puttygen.exe**, and log in using the `.ppk` key file
- Set password for root (on the remote machine):

```
sudo passwd
```

2. Environment Setup

In this assignment, you need to install several packages for later development. Specifically, **Apache** for web server, **MySQL** or **SQLite** for database, and **PHP** for server backend.

2.1 Install Required Packages

1. Install PHP

```
sudo amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
```

2. Install MySQL and Apache

```
sudo yum install -y httpd mariadb-server
```

3. Start Apache

```
sudo systemctl start httpd
```

If you type your IP address in the browser, you will get an error because you have not opened port 80.

For more information, please check the following website:

Tutorial: Install a LAMP web server on Amazon Linux 2: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-lamp-amazon-linux-2.html

2.2 Config File Permissions

1. Add your user to the Apache group

```
sudo usermod -a -G apache ec2-user
```

2. Set group ownership of the web folder to the Apache group

```
sudo chown -R ec2-user:apache /var/www
```

3. Add group write permissions and set the group ID

```
sudo chmod 2775 /var/www && find /var/www -type d -exec sudo chmod 2775 {} \;
```

4. Add group write permissions of the web folder and its subdirectories

```
find /var/www -type f -exec sudo chmod 0664 {} \;
```

For more information, please check the following website:

Tutorial: Install a LAMP web server on Amazon Linux 2: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-lamp-amazon-linux-2.html

2.3 Test LAMP Server

Type the following command to create the `phpinfo.php` page in `/var/www/html/`

```
echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
```

If you type `http://[server IP address]/phpinfo.php` in the browser, you will get an error because you have not opened port 80.

2.4 Apache Configuration

- `httpd.conf`
  - Location: `/etc/httpd/conf/httpd.conf`
  - If you don't know how to modify, leave it unchanged
- Some Parameters
  - `ServerRoot "/etc/httpd"`: Define the root folder of Apache service
  - `Listen 80`: Apache server will listen to port 80 for request
  - `DocumentRoot "/var/www/html"`: Where your webpages are placed
  - `KeepAlive On`: Allow persistent connections (default)
  - `MaxKeepAliveRequests 500`: Set the max number of requests during a persistent connection

For more information, please check the following website:

Apache Core Features: https://httpd.apache.org/docs/2.4/mod/core.html

2.5 PHP Configuration

- `php.ini`
  - Location: `/etc/php.ini`
- Some Parameters
  - `file_uploads = On`: Whether or not to allow http file uploads

    - `display_errors = Off`: Whether the error message will be displayed on the screen
    - `display_startup_errors = Off`: Whether the error message in the initialization process will be showed
    - `log_errors = On`: Whether the error messages will be logged

For more information, please check the following website:

List of `php.ini` Directives: https://www.php.net/manual/en/ini.list.php

3. Security Configuration

- Open necessary ports only, i.e., 22 and 80 for now, 443 in later phases
    - You may visit the previous links now
- Upgrade the packages regularly
- Hide the versions of everything in HTTP headers
    - OS, Apache, PHP, ...
    - `ServerTokens` in `httpd.conf`
- Disable directory index in Apache
- Do not display any PHP warnings/errors to end-users
    - By configuring the file `php.ini`